11 10 9 8 6 5 4 3

12

c_1 c_2 c_{n-2} c_{n-1}

x x^2 x^{n-1} x^n

R_1 R_2 R_{n-1} R_n

2 14 13 3

1 1

Fig. 1

$$T^N = \begin{pmatrix} (t_{1,k})_{k=1,2,..,n} \\ (t_{2,k})_{k=1,2,..,n} \\ \vdots \\ (t_{n,k})_{k=1,2,..,n} \end{pmatrix} = \begin{pmatrix} [x^N] \bmod f^* \\ [x^{N+1}] \bmod f^* \\ \vdots \\ [x^{N+n-1}] \bmod f^* \end{pmatrix}$$

Fig. 2

Desired offset	Previous method	Method described above
100	100	660
1,000	1,000	1,000
10,000	10,000	1,400
50,000	50,000	1,600
100,000	100,000	1,750
200,000	200,000	1,860

Fig. 3